

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

JACKSON ALEXANDER COSKO,

Defendant.

Case No. 18-CR-303 (TFH)

STATEMENT OF OFFENSE IN SUPPORT OF GUILTY PLEA

Summary of the Plea Agreement

Defendant Jackson Alexander Cosko agrees to admit guilt and enter a plea of guilty to a Superseding Information, which charges two counts of Making Public Restricted Personal Information, in violation of 18 U.S.C. § 119, one count of Computer Fraud, in violation of 18 U.S.C. § 1030(a)(2), one count of Witness Tampering, in violation of 18 U.S.C. § 1512(b)(3), and one count of Obstruction of Justice, in violation of 18 U.S.C. § 1512(b)(2)(B).

I. Elements of the Offenses

A. Making Public Restricted Personal Information (Counts One and Two)

The elements of Making Public Restricted Personal Information, in violation of 18 U.S.C. § 119, are:

First, that the defendant knowingly made restricted personal information publically available;

Second, that the information was about a covered person, or a member of the immediate family of that covered person;

Third, that the defendant did so with the intent to intimidate, or with the intent and knowledge that the restricted personal information would be used by others to intimidate, a covered person or a member of the immediate family of that covered person.

A United States Senator is a "covered person" under 18 U.S.C. § 119(b)(2)(A) (cross reference to 18 U.S.C. § 1114).

B. Computer Fraud (Count Three)

The elements of Computer Fraud, in violation of 18 U.S.C. §§ 1030(a)(2) and (c)(2)(B)(ii), are:

First, that the defendant accessed a protected computer without authorization;

Second, that the defendant thereby obtained information from any department or agency of the United States; and

Third, that the defendant did so intentionally; and

Fourth, that the defendant committed the offense in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, including an act in violation of 18 U.S.C. § 1028(a)(7).

C. Witness Tampering (Count Four)

The elements of Witness Tampering, in violation of 18 U.S.C. § 1512(b)(3), are:

First, that the defendant knowingly intimidated, threatened, or corruptly persuaded another person (or attempted to do so);

Second, that the defendant did so with the intent to hinder, delay, or prevent communicating to a law enforcement officer;

Third, the communication sought to be prevented related to the commission or possible commission of a Federal offense, which includes computer fraud.

D. Obstruction of Justice (Count Five)

The elements of Obstruction of Justice, in violation of 18 U.S.C. § 1512(b)(2)(B), are:

First, the defendant altered, destroyed, mutilated or concealed a record, document or other object (or attempted to do so);

Second, the defendant acted knowingly;

Third, the defendant acted corruptly; and

Fourth, the defendant acted with the intent to impair the object's integrity or availability for use in an official proceeding.

Both a grand jury investigation and a trial hearing are official proceedings, 18 U.S.C. §1512(g)(1), and neither need not be pending or about to be instituted at the time of offense. 18 U.S.C. §1512(f).

II. Brief Statement of Facts

a. The Defendant's Termination

In May 2018, the defendant was terminated from his employment with United States Senator Maggie Hassan. Prior to his termination, the defendant had served as a computer systems administrator in the Office of Senator Hassan. In that position, the defendant had an intimate knowledge of, and broad access to, the computer systems, administrative accounts, and related security measures (including passwords and usernames) in Senator Hassan's Office. When the defendant was terminated, his right of access to Senator Hassan's Office and computer systems was terminated. After his termination, the defendant knew that he had no right to enter the

Senator's Office unescorted and without authorization, or to access any computers in the Senator's Office.

b. Overview of The Defendant's Burglaries, Computer Fraud, & Data Theft

The defendant was angry about his termination and concerned that it would have an adverse impact on his prospects for future employment. As a result, beginning no later than July 2018 and continuing until October 2018, the defendant engaged in an extensive computer fraud and data theft scheme that he carried out by repeatedly burglarizing Senator Hassan's Office. The defendant engaged in an extraordinarily extensive data-theft scheme, copying entire network drives, sorting and organizing sensitive data, and exploring ways to use that data to his benefit.

The defendant broke into Senator Hassan's Office on at least four occasions, including on or about July 26, 2018, August 6, 2018, and October 2, 2018. The defendant gained access to Senator Hassan's Office by unlawfully obtaining keys from a staffer who was (at the time) still employed in the Office ("SUBJECT A"). The defendant then used those keys to enter the Senator's Office alone at night, with the specific intent of unlawfully accessing Senate-owned computers, for the express purpose of stealing electronic information – including login credentials and other means of identification belonging to Senate employees. On at least one occasion, on October 2, 2018, the defendant obtained the keys from SUBJECT A with SUBJECT A's knowledge that the defendant was using the keys to illegally enter the Senator's Office.

During his repeated burglaries of Senator Hassan's Office, the defendant obtained dozens of means of identification (including network login credentials) belonging to at least six employees of the Office of Senator Hassan. In order to accomplish that goal, the defendant surreptitiously installed "keylogger" devices on at least six computers in Senator Hassan's Office. The

keylogger devices were designed to be unobtrusive, legitimate looking devices that would go unnoticed by the individuals that were using the affected computers. They were also designed to record the keystrokes that Senate staffers typed on their Senate-owned computers – including the keystrokes that comprised usernames and passwords for Senate computers and computer networks.

During burglaries after the installation of the keyloggers, the defendant accessed the keylogger devices and obtained the information they had recorded. The defendant was thus able to identify the login credentials that provided access to Senate computers and computer networks. The defendant then fraudulently used those stolen login credentials, unlawfully accessed Senate computers and computer networks, and then stole data (including dozens of additional login credentials for other electronic accounts) belonging to Senator Hassan's Office or its employees.

During the burglaries, the defendant copied dozens of gigabytes of data from computers in Senator Hassan's Office, including dozens of usernames and passwords belonging to Senate employees, credit card information belonging to Senate employees, social security numbers belonging to Senate employees, personally identifying information ("PII") belonging to hundreds of other persons, and tens of thousands of e-mails and internal documents belonging to Senator Hassan's Office. The defendant also obtained contact information for numerous sitting U.S. Senators, which included their home addresses and private phone numbers.

The defendant copied that data onto multiple computers and electronic storage devices. The defendant sorted and organized at least some of the data, including by compiling one electronic folder that he designated as "high value." This "high value" folder included, among other items, the personal home addresses of multiple Senators.

c. The Defendant's Doxxing Offenses¹

On September 27, 2018, while watching the televised broadcast of a United States Senate hearing concerning the nomination of a United States Supreme Court Justice, the defendant became angry at some of participants in the hearing – and he acted on that anger by maliciously publishing the personal home addresses and telephone numbers of Senators Lindsay Graham, Orrin Hatch, and Mike Lee. The defendant published that information maliciously, with the intent to intimidate the Senators, and with the knowledge and intent that others who learned of the information would then use the information to intimidate the three aforementioned Senators, as well as members of their immediate families, by using the information that the defendant had now made public.

Specifically, between about 5:15 p.m. and 5:55 p.m., the defendant used a computer that was connected to the internet through a facility maintained by the House of Representatives and visited the “Wikipedia” articles for each of those Senators. The defendant then edited those Wikipedia articles – which were publicly available over the internet – so that the articles would include the Senators’ home addresses and telephone numbers. The defendant also helped publicize those edits, by posting or “re-tweeting” posts about his edits over Twitter.

During the next few days, after news organizations reported on the publication of the above-listed Senators’ personal information (and described the impact that the publication had upon the Senators and their family members), Senator Rand Paul called for an investigation of those offenses. The defendant responded by maliciously publishing the personal home addresses

¹ “Doxxing” is the act of publishing private or identifying information about an individual on the Internet, typically with malicious intent.

and telephone numbers of Senator Paul as well as Senate Majority Leader Mitch McConnell, with the intent to intimidate them, and with the knowledge and intent that others would use that information to intimidate Senators Paul and McConnell. Specifically, on October 1, 2018, at about 5:50 p.m., using a computer that was connected to the internet through a facility maintained by the Senate, the defendant edited a "Wikipedia" article so that it would include Senator Paul's home address and phone number, as well the text, "He dares call for an investigation of ME?!?!?!? ... I am the Golden God! ... Also It's my legal right as an American to post his info ... We are malicious and hostile ... Send us bitcoins ... Wednesday night will be the doxxed next[.]"

Similarly, a few minutes later, using the same computer and internet connection, the defendant published the home address and telephone number of Senator Mitch McConnell.

The home addresses and telephone numbers that the defendant published constituted "restricted personal information" under 18 U.S.C. § 119, and the defendant obtained that restricted personal information by means of the burglaries and unlawful access to Senate computers described above.

d. The Defendant's Final Burglary & Subsequent Obstruction of Justice

On October 2, 2018, the defendant obtained SUBJECT A's key to Senator Hassan's Office from SUBJECT A, who provided the defendant the keys knowing that the defendant intended to unlawfully enter the Senator's Office that night with SUBJECT A's keys. Shortly after 10:10 p.m., the defendant used SUBJECT A's key to open the locked office door of Senator Hassan's Office. Once inside, the defendant planned on unlawfully accessing a Senate-owned computer that was used by Witness 3, an employee of Senator Hassan. When the defendant entered the office, he went to Witness 3's computer, used Witness 3's login credentials (which the defendant had

previously stolen), and logged in to Witness 3's computer. The defendant opened a web-based e-mail application, which Witness 3 had never used, and attempted to review Witness 3's e-mails.

Shortly thereafter, while the defendant was typing at Witness 3's keyboard and unlawfully accessing Witness 3's computer, Witness 2 entered Senator Hassan's Office, and immediately recognized the defendant as a person who did not have authority to be inside the Senator's Office. The defendant used Witness 3's keyboard, locked Witness 3's computer, and fled. A few minutes later, at 10:25 p.m., the defendant sent a threatening e-mail to Witness 2. The defendant sent the e-mail from the address livefreeorpwn@gmail.com, an e-mail address that the defendant had created to conceal his true identity, including in connection with other activities involving data that the defendant had stolen from Senator Hassan's Office. The e-mail to Witness 2 was directed to Witness 2's email account at Senator Hassan's Office, and was titled, "I own EVERYTHING." The body of the e-mail stated, "If you tell anyone I will leak it all. Emails signal conversations gmails. Senators children's health information and socials." The defendant's reference to "signal conversations" was a reference to the use of Signal, a popular messaging application which enables chats/conversations. The defendant's reference to "socials" was a reference to social security numbers.

Later that evening, after the defendant had returned home, the defendant began to plan to destroy and conceal evidence of his crimes. The defendant wrote a note, reminding himself to "Backup all files . . . Mail backup . . . Burn aliases . . . Wipe down comps[.]" The defendant then attempted to actually delete electronic evidence, including electronic evidence of his data theft from Senator Hassan's Office, as well as evidence of his doxxing offenses. The items that the

defendant deleted data from included a laptop computer that the defendant had used to "dox" the other Senators, and which he used to obtain and download stolen data from the Senator's Office.

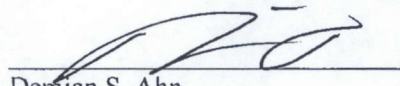
The following morning, on October 3, 2018, the defendant met with SUBJECT A, to return SUBJECT A's key. During their meeting, and consistent with his handwritten note, the defendant told SUBJECT A to wipe down all of the computers, keyboards and computer mice, and to unplug the computers in Senator Hassan's Office. SUBJECT A understood, and the defendant hoped, that these actions would destroy latent fingerprints as well as electronic evidence of his unlawful conduct, and prevent them from being available for any criminal and grand jury investigation. SUBJECT A, who knew that the defendant had unlawfully entered Senator Hassan's Office the night before, did in fact "wipe down" computer keyboards and computer mouse devices, but was unable to complete the task of unplugging the computers, because Witness 3 entered the Office. SUBJECT A then texted the defendant, at about 8:28 a.m. on October 3, 2018, stating, "Hey[.] So I was able to wipe down the keys and mouse but [Witness 3] was coming so I could [not] do the other thing[.]" The defendant replied, "Thanks," and SUBJECT A finished the conversation by responding, "Np, sorry I couldn't do everything."

Respectfully submitted,

ALESSIO D. EVANGELISTA

Attorney for the United States, Acting Under
Authority Conferred by 28 U.S.C. § 515

BY:


Demian S. Ahn

Tejpal S. Chawla

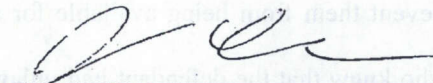
Assistant United States Attorneys

DEFENDANT'S ACKNOWLEDGMENT

I have read each of the 10 pages constituting this Statement of Offense and Acknowledgment, understand it, and agree that it is true and accurate. While it is not a complete recitation of everything that I did or everything that I know, it accurately describes my conduct and my knowledge concerning my own involvement in the illegal activity that is the subject of this Statement of Offense. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this factual proffer fully.

Date:

3/25/19



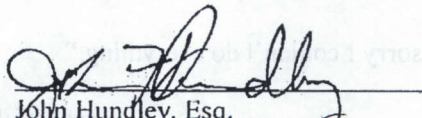
Jackson Alexander Cosko
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read each of the 10 pages constituting this Statement of Offense and Acknowledgement, reviewed them with my client, and discussed it with my client.

Date:

3/25/19



John Hundley, Esq.
Christopher Hatfield, Esq.
Brian Stolarz, Esq.
Attorneys for Defendant